

Reply to: ‘Reply to: “Comment on: ‘How much security does Y-00 protocol provide us?’”’

Ranjith Nair, Horace P. Yuen, Eric Corndorf, Prem Kumar

*Center for Photonic Communication and Computing
Department of Electrical and Computer Engineering
Department of Physics and Astronomy
Northwestern University, Evanston, IL 60208*

Abstract

Nishioka *et al* claim in [1], elaborating on their earlier paper [2], that the direct encryption scheme called Y-00 [3,4] is equivalent to a classical non-random additive stream cipher, and thus offers no more security than the latter. In this paper, we show that this claim is false and that Y-00 may be considered equivalent to a *random* cipher. We explain why a random cipher provides additional security compared to its nonrandom counterpart. Some criticisms in [1] on the use of Y-00 for key generation are also briefly responded to.

Key words: Quantum cryptography
PACS: 03.67.Dd

1 Introduction

The direct encryption system called Y-00 or $\alpha\eta$ [3,4] uses coherent states to transmit encrypted information between two users, Alice and Bob, sharing a secret key. Nishioka *et al* claimed in [2] that the security of Y-00 was completely equivalent to that of a classical non-random additive stream cipher. Although we rebutted this claim in [5], the authors of [2] have replied in [1] to the effect that we did not understand the claims made in their original paper, and that our reply was irrelevant. It is in fact true that some details of our understanding of the claims in [2] differ from the purported clarifications of the

Email address: r-nair@northwestern.edu (Ranjith Nair).

same provided in [1]. However, setting aside questions of clarity of the claims in [2], we understand their claims in [1] exactly and contend that the claimed equivalence of Y-00 to a classical non-random additive stream cipher is false, thus reiterating the conclusion of [5]. We provide arguments in this paper that conclusively demonstrate that Y-00 is not equivalent to a non-random cipher.

In Section 2, we briefly review the Y-00 direct encryption protocol. In Section 3, we describe the claims in [2] and [1]. In Section 4, we review the concept of a random cipher and describe why they are more secure than non-random ones against attacks on the key, thus highlighting the added feature that Y-00 provides over a non-random cipher. We then rebut the claims in [1] and show why Y-00 is not equivalent to a non-random stream cipher. In Section 5, we briefly respond to the criticisms in [1] of using Y-00 with weak coherent states as a key generation system.

2 The Y-00 Direct Encryption Protocol

We review the Y-00 protocol, using the notations of [1] for easy reference.

- (1) Alice and Bob share a secret key \mathbf{K}_s .
- (2) Using a pseudo-random-number generator $PRNG(\cdot)$, e.g., a linear feedback shift register, the seed key \mathbf{K}_s is expanded into a running key sequence $\mathbf{K} = PRNG(\mathbf{K}_s) = (K_1, \dots, K_N)$, with each block $K_i \in \{0, 1, \dots, M-1\}$.
- (3) For each bit r_i of a plaintext sequence $\mathbf{R}_N = (r_1, \dots, r_N)$, Alice transmits the coherent state

$$|\psi(K_i, r_i)\rangle = |\alpha e^{i\theta(K_i, r_i)}\rangle, \quad (1)$$

where $\alpha \in \mathbb{R}$ and $\theta(K_i, r_i) = [K_i/M + (r_i \oplus \Pi(K_i))]\pi$. $\Pi(K_i) = 0$ or 1 according to whether K_i is even or odd. This distribution of possible states is shown in Fig. 1. Thus K_i can be thought of as choosing a ‘basis’ with the states representing bits 0 and 1 as its end points.

- (4) Bob, knowing K_i , makes a measurement to discriminate just the two states $|\psi(K_i, r_i)\rangle$ and $|\psi(K_i, r_i \oplus 1)\rangle$.

The probability that Bob makes an error can be made negligibly small by choosing the mean photon number $S \equiv |\alpha|^2$ large enough. In particular, the optimal quantum measurement [6] for Bob has error probability

$$P_e^B \sim \frac{1}{4} \exp(-4S). \quad (2)$$

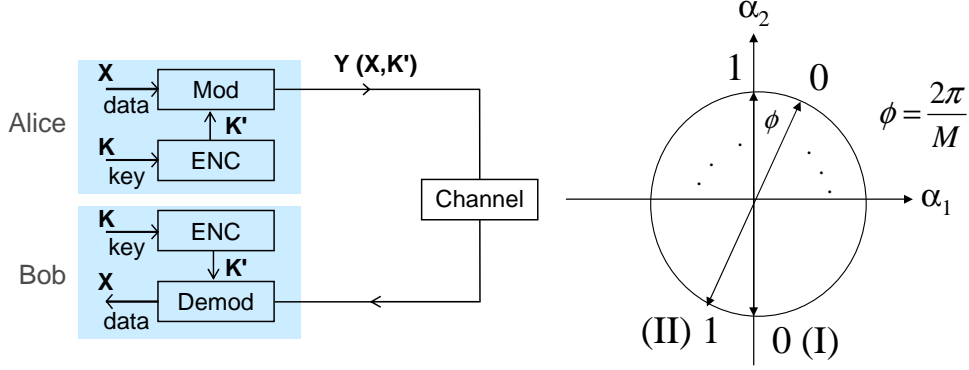


Fig. 1. Left: Overall schematic of the $\alpha\eta$ scheme. Right: Depiction of $M/2$ bases with interleaved logical state mappings.

Eve, not knowing K_i , is faced with the problem of distinguishing the density operators ρ^0 and ρ^1 where

$$\rho^b = \sum_{K_i} \frac{1}{M} |\psi(K_i, b)\rangle \langle \psi(K_i, b)|. \quad (3)$$

For a fixed signal energy S , Eve's optimal error probability is numerically seen to go asymptotically to $1/2$ as the number of bases $M \rightarrow \infty$ (See Fig. 1 of [3]). The intuitive reason for this is that increasing M more closely interleaves the states on the circle representing bit 0 and bit 1, making them less distinguishable. Therefore, at least under *individual* attacks on each qumode, the Y-00 protocol offers any desired level of security determined by the relative values of S and M .

One can also ask if Eve can obtain the key \mathbf{K}_s under a *known-plaintext* attack, thus compromising the security of future data. While the complete analysis of the security of Y-00 under known-plaintext analysis has not been performed, we can still make some remarks about the security that Y-00 offers against an attack involving a fixed measurement (e.g., a heterodyne or phase measurement) on each qumode followed by a *brute-force trial* of remaining key candidates. Indeed, a simple estimate of the noise in the phase measurement (which performs better than the heterodyne measurement) can be obtained by assuming that the noise moves the measured angle around the transmitted value uniformly within a standard deviation $1/|\alpha|$ of the measurement noise. Then, it is seen that the number of possible bases N_σ consistent with the known bit b in each measurement is $N_\sigma = M/(2\pi|\alpha|)$. Thus, the randomization provided by the quantum noise creates a search problem for Eve that would *not* be present if Y-00 was a non-random cipher.

3 Claims in Nishioka *et al* [1]

Nishioka *et al* claim that Y-00 can be reduced to a classical non-random stream cipher under the attack that we now review. For each transmission i , Eve makes a heterodyne measurement on the state and collapses the outcomes to one of $2M$ possible values. Thus, the outcome $j \in \{0, \dots, 2M-1\}$ is obtained if the heterodyne result falls in the wedge for which the phase $\theta \in [\theta_j - \pi/2M, \theta_j + \pi/2M]$, where $\theta_j = \pi j/M$. Further, for $q \in \{0, \dots, M-1\}$ representing the M possible values of each K_i , Nishioka *et al* construct a function $F_j(q)$ with the property that, for each i , and the corresponding running key value K_i actually used,

$$F_{j(i)}(K_i) = r_i \quad (4)$$

with probability very close to 1. In fact, for the parameters $S = 100$ and $M = 200$, they calculate the probability that Eq.(4) fails to hold to be 10^{-44} , which value they demonstrate to be negligible for any practical purpose.

The authors of [1] further claim that the above function $F_{j(i)}(q)$ can always be represented as the XOR of two bit functions $G_{j(i)}(q)$ and $l_{j(i)}$, where $l_{j(i)}$ depends *only* on the measurement result. Thus, they make the claim that the equation

$$l_{j(i)} = r_i \oplus G_{j(i)}(K_i) \quad (5)$$

holds with probability effectively equal to 1. They then observe that a classical additive stream cipher [7,8] (which is non-random by definition) satisfies

$$l_i = r_i \oplus \tilde{k}_i, \quad (6)$$

where r_i , l_i , and \tilde{k}_i are respectively the i th plaintext bit, ciphertext bit and running key bit. Here, \tilde{k}_i is obtained by using a seed key in a pseudo-random-number generator to generate a longer running key. The authors of [1] then argue that since $l_{j(i)}$ in Eq.(5), like the l_i in Eq.(6), depends just on the measurement result, the validity of Eq.(5) proves that the security of Y-00 is equivalent to that of a classical stream cipher. In particular, they claim that by interpreting $l_{j(i)}$ as the ciphertext, Y-00 is not a random cipher, i.e., it does not satisfy Eq.(7) of the next section.

We analyze and respond to these claims and other statements in [1] in the following section.

4 Reply to claims in [1]

First of all, we review the definition of a *random* cipher. Such a cipher is called a ‘privately-randomized cipher’ in [8], but we will call it just a random cipher. A random cipher is defined by the two conditions:

$$H(Y_N|\mathbf{K}_s, R_N) \neq 0, \quad (7)$$

and

$$H(R_N|Y_N, \mathbf{K}_s) = 0. \quad (8)$$

Here, Y_N refers to the N – symbol long ciphertext and R_N and \mathbf{K}_s are the plaintext and secret key, as in section 1. Note that there is no restriction on the alphabet of Y_N , which may be binary, M -ary or even continuous. Eq.(7) implies that, for a given key, the plaintext may be mapped by the encrypter into more than one possible ciphertext. However, it is still required that the plaintext can be recovered from the ciphertext and the key, which is the meaning of Eq.(8). The case where Eq.(8) holds but Eq.(7) does not is the usual case of a non-random cipher in standard cryptography.

The advantage of a random cipher, which is briefly described in [5] but not appreciated in [1], is that it may be secure against attacks on the key in the case when the attacker knows the statistics $p(R_N)$ of the data. In the case where the r_i are independent and identically distributed, a random cipher can be constructed that provides complete information-theoretic security of the key [9], in the sense that $H(\mathbf{K}_s|Y_N) = H(\mathbf{K}_s)$. Such security cannot be obtained with nonrandom ciphers [10]. See [10] for a detailed discussion on the security of random ciphers. Although we do not claim such information-theoretic security for Y-00, the possibility is not ruled out. We have already commented on the added brute-force search complexity of Y-00 against attacks on the key in Section 2. We now proceed to prove that the claim in [1] that Y-00 is reducible for Eve to a non-random stream cipher under a heterodyne measurement is false.

To begin with, we believe that Eq. (4) (Eq. (14) in [1]) is correct with the probability given by them. The content of this equation is simply that Eve is able to decrypt the transmitted bit from her measurement data J_N and the key \mathbf{K}_s . In other words, it merely asserts that Eq.(8) holds for $Y_N = J_N$. As such, it does not contradict, and is even *necessary*, for the claim that Y-00 is a random cipher for Eve. In fact, we already claimed in [4] and [5] that such a condition holds. In this regard, note also that the statement in Section 4.1 of [1] that “informational secure key generation is impossible when (Eq.(4)

of this paper) holds” is irrelevant, since direct encryption rather than key generation is being considered here.

We also agree with the claim of Nishioka *et al* that it is possible to find functions $l_{j^{(i)}}$ and $G_{j^{(i)}}(q)$, the former depending only of the measurement result $j^{(i)}$, such that Eq.(5) holds, again with probability effectively equal to one. The error in [1] is to use this equation to claim, in analogy with Eq. (6), that Y-00 is reducible to a classical stream cipher, and hence non-random.

To understand the error in their argument, note that, for Eq. (6) to represent an *additive* stream cipher, the l_i in that equation should be a function *only* of the measurement result, and \tilde{k}_i should be a function *only* of the running key. While the former requirement is true also for the $l_{j^{(i)}}$ in Eq. (5), the latter is certainly *false* for the function $G_{j^{(i)}}(K_i)$ in Eq. (5), since it depends *both* on the measurement result $j^{(i)}$ and the running key K_i . Indeed, it can be seen that the definition of the function $F_{j^{(i)}}(K_i)$, and thus, $G_{j^{(i)}}(q)$ depends on the sets $C_{j^{(i)}}^+$ and $C_{j^{(i)}}^-$ defined in Eq. (12) of [1]. The identity of these sets in turn depends on the relative angle between the basis q and Eve’s estimated basis $\tilde{j}^{(i)} = j^{(i)} \bmod M$. Thus, it is clearly the case that $G_{j^{(i)}}(K_i)$ must depend both on $j^{(i)}$ and K_i , a fact also revealed by the inclusion of the subscript $j^{(i)}$ by the authors of [1] in the notation for G .

We have shown above why the representation of Y-00 via Eq. (5) is not equivalent to an additive stream cipher. The question may be raised, however, if Eq. (5) reduces Y-00 to any kind of nonrandom cipher whatsoever. We will show below that the answer is negative. Indeed, Nishioka *et al* emphasize that Y-00 is nonrandom because

$$H(L_N | R_N, \mathbf{K}_s) = 0 \quad (9)$$

holds, where $\mathbf{L}_N = (l_{j^{(1)}}, \dots, l_{j^{(N)}})$. This equation follows from Eq. (5) and so by considering $\mathbf{L}_N \equiv Y_N$ to be the ciphertext, the Eq.(7) is not satisfied, thus supposedly making Y-00 nonrandom. The choice of \mathbf{L}_N as the ciphertext is supported by the statement in [1] that “It is a matter of preference what we should refer to as “ciphertext”.” This is not true without qualification. It ignores the *crucial* point that the random variable that is chosen as ciphertext must be sufficient to decrypt to the corresponding R_N for every value of the key. We will show below that, for Y-00, the ciphertext alphabet needs to be atleast $(2M)$ -ary, although larger, even continuous alphabets (such as the possible values of phase angle in a phase measurement or the two quadrature amplitudes in a heterodyne measurement) may be used. Thus, if one wants to claim equivalence to a classical cipher (random or non-random), for a particular choice of ciphertext Y_N , one must show that Eq. (8) is satisfied using that *same* ciphertext Y_N . In the case where $Y_N = \mathbf{L}_N$, one may readily see

that Eq. (8) is not satisfied, i.e., $H(\mathbf{R}_N|\mathbf{L}_N, \mathbf{K}_s) \neq 0$. The reason is that, as we noted in our description above of the function $G_{j^{(i)}}(q)$, decrypting r_i requires knowledge of certain ranges in which the angle between the basis chosen by the running key and the estimated basis $j^{(i)}$ falls. To convey this information *for every possible* $j^{(i)}$, one needs at least $\log_2(2M)$ bits. It follows that the single bit $l_{j^{(i)}}$ is insufficient for the purpose of decryption, and so Eq. (8) cannot be satisfied for $Y_N = \mathbf{L}_N$. Therefore, we conclude, that in the interpretation of \mathbf{L}_N as the ciphertext, decryption is not possible even if Eve has the key \mathbf{K}_s . Indeed, it is \mathbf{J}_N that can be regarded as a possible ciphertext, since Eq. (8) is satisfied for $Y_N = \mathbf{J}_N$. The fact that \mathbf{J}_N is a true ciphertext sufficient for decryption is implicit in the dependence on $j^{(i)}$ of the function G in Eq. (5). However, with this choice of ciphertext, Y-00 necessarily becomes a *random* cipher, because $H(\mathbf{J}_N|\mathbf{R}_N, \mathbf{K}_s) \neq 0$ – this latter fact is admitted by Nishioka *et al* in [1].

We hope that the discussion above makes it clear that the ‘reduction’ of Y-00 in [1] to a non-random cipher is false, and that in fact, no such reduction can be made under the heterodyne attack considered in [1]. However, the representation of ciphertext by $Y_N = \mathbf{J}_N$ does reduce it to a *random* cipher under the heterodyne attack. As a result, it can be implemented classically in principle, but not in practice. This is because true random numbers can only be generated physically, not by an algorithm, and the practical rate for such generation is many orders of magnitude below the \sim Gbps rate in our experiments where the coherent-state quantum noise does the randomization *automatically*. Furthermore, our physical “analog” scheme does not sacrifice bandwidth or data rate compared to other known randomization techniques. See [10] for a detailed discussion.

We conclude this section by responding to some other statements made in [1].

In Section 3.2, Nishioka *et al* state that “It is interesting to note that a smaller M (but not $M=1$) is preferable for increasing the stochastic property.” Here, they mean that the decryption using \mathbf{J}_N and the key is noisier for smaller M . We claim that this cannot be the case and that the decryption probability is essentially independent of M . In any case, for the heterodyne quantum noise to cover more states on the circle, it is clear that a larger M is preferable (See our discussion in Section 2).

In Section 3.3, Nishioka *et al* claim that “The value of $l_{j^{(i)}}$ does not have to be the same as that of $l_{j^{(i')}}$ when $i \neq i'$, even if $j^{(i)} = j^{(i')}$ holds.” This statement is in direct contradiction to their previous statement in the same subsection that “ $l_{j^{(i)}}$ depends only on the measurement value $j^{(i)}$ ”.

In the same subsection, Nishioka *et al* claim that “In ([2]), we showed another concrete construction of $l_{j^{(i)}}$...”. In our opinion, there was no explicit con-

struction of $l_{j(i)}$ in that paper, which to us seemed quite vague. We were led to the choice of l_i described in [5] by the attempt to make the additive stream cipher representation Eq. (6) valid. In fact, such a representation is claimed by Nishioka *et al* in their Case 2 of [2]. It turned out, however, that decryption using that l_i suffered a 0.1 – 1% error depending on the value of S used. See [5] for further details. In any case, as we have shown above, no construction of a single-bit from the heterodyne measurement results can satisfy Eq.(8) with the extremely low probability given in [1].

5 Remarks regarding Key Generation using Y-00

In [5], we replied to the claim that information-theoretically secure key generation is impossible for Y-00 by showing a 6 dB advantage that the users have over Eve launching a heterodyne attack. This advantage can be used for practical key generation using a small enough value of S . This is acknowledged in [1], thus validating our claim that it is indeed possible. However, the new issue is raised in [1] that this advantage is too small to allow Y-00 to generate keys, in their example, over a distance of 50 km. In this connection, we merely wish to state that, (i) this is not the original issue under dispute and we do not wish to bring a new issue into the present discussion; (ii) similar loss limits are also present for BB84; (iii) other techniques and schemes are already discussed in [4] to overcome this distance limit.

6 Conclusion

We have demonstrated that, under a heterodyne measurement, the Y-00 Direct Encryption protocol cannot be reduced to a classical non-random stream cipher, as claimed in [1]. Its security under heterodyne attack is equivalent to a corresponding random cipher.

References

- [1] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, H. Imai, Reply to: “Comment on ‘How much security does Y-00 protocol provide us?’”, To appear in Phys. Lett. A (2005).
- [2] T. Nishioka, T. Hasegawa, H. Ishizuka, K. Imafuku, H. Imai, How much security does Y-00 protocol provide us?, Phys. Lett. A 327 (2004) 28-32; quant-ph/0310168.

- [3] G. Barbosa, E. Corndorf, P. Kumar, H. Yuen, “Secure communication using mesoscopic coherent states”, Phys. Rev. Lett. 90 (2003) 227901.
- [4] H. Yuen, KCQ: A new approach to quantum cryptography I. General principles and qumode key generation, quant-ph/0311061.
- [5] H.P. Yuen, P. Kumar, E. Corndorf, R. Nair, “Comment on ‘How much security does Y-00 protocol provide us?’”, quant-ph/0407067, To appear in Phys. Lett. A (2005).
- [6] C. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, 1976.
- [7] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
- [8] J.L. Massey, An introduction to contemporary cryptology, Proc. IEEE, 76 (1988) 533-549.
- [9] Ch.G. Gunther, “A universal algorithm for homophonic coding”, Advances in Cryptology - EUROCRYPT '88, Lect. Notes in Comp. Sci 330, 405-414, Springer-Verlag.
- [10] H.P. Yuen, R. Nair, E. Corndorf, P. Kumar, and G.S. Kanter, On the security of $\alpha\eta$: Response to ‘Some attacks on quantum-based cryptographic protocols’ , Submitted to QIC; quant-ph/0509091.